Published and Copyright (c) 1999 - 2016
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1828 07/15/16

~ TP-Link Loses Domains! ~ People Are Talking! ~ Natcar Racing Game!
~ Game Boy Games Released ~ OLD Printer Bug Fixed ~ Weird CFAA Rulings!
~ DARPA Challenges Hackers ~ More Charges for Fed! ~ NES Is Next Console!

~ Facebook’s OpenCellular! ~ ~ Microsoft Appeal Win

-* Guide to GEM Coding with AHCC *-
-* Snowden Says A Dark Day for Russia! *-
-* Bulgaria Passes Law for Government Software *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

And the atrocities continue, with the latest occurring in France this week. Time will tell what kind of "hatred" this latest terrorist (or perceived terrorist) had that led him to take so many innocent lives. Earlier today I heard one newscaster ask another "...when will this madness stop?" The answer is quite simple: Never! As long as there are extremists in the world, those with ideologies filled with hatred, these kinds of acts will continue to occur all over the world.

Quickly changing gears, to a much lighter note... I don’t usually talk about "apps" and gaming on tablet devices and/or phones because they don’t come across (at least in my mind) as real computing or gaming as I know it. Yes, I’m sure one can argue with me that there’s no real difference simply because of the type of platform used, but I’m more of a traditionalist when it comes to this stuff.

However, I will briefly mention the latest phenomenon - the newest gaming app that has generated worldwide attention lately: Pokemon Go. Whether or not the game is getting a lot more attention because of the lack of judgment by some players, or the games is really a lot of fun - I don’t know. People are getting hurt and killed because of their own stupidity and carelessness. Some people simply cannot walk and chew gum at the same time - an adage from my childhood days! There’s a sound reason why there are laws that say you cannot text and drive - it’s unsafe. Walking around outside - regardless of the setting - can be dangerous if you’re constantly doing so with your phone in front of your face!

I haven’t played the game, yet. I do plan to download it to see what all of the hype is about. With temperatures here in the 90’s, I don’t have any immediate plans to wander around town looking for Pokemon characters! But, I like the premise of the game; it reminds me of taking part in scavenger hunts when I was a lot younger. We’ll see what happens over the next couple of weeks! Regardless, be responsible and be safe while playing!

Until next time...

=~=~=~=

Guide to GEM Coding with AHCC

I put together some notes to remind myself how my GEM programs are working. Most of this comes from CManShip, and things I learnt [sic] working through a lot of my own misunderstandings. I've also been helped along at times by members of this forum. These notes try to put this information together in one place, and may be useful to anyone else learning how to write GEM programs using AHCC. So far, I have only covered how to work with windows.

The notes are in the form of a pdf document: http://peterlane.info/downloads/guide.pdf. I work through a series of progressively more complex versions of a sample program - the source code for these versions: http://peterlane.info/downloads/guide-source.zip The examples have been tested on a Firebee and an Atari ST.

Let me know if anything's unclear, or could be improved.

Enjoy!
Peter Lane
Firebee | STE (4Mb, TOS 2.06)
http://peterlane.info/firebee.html

Natcar

Hi!

Just wanted to say that we have released a demo of Natcar, a Supercars inspired racing game! :D It is available at nature.atari.org.

It requires a SuperVidel, running at a 720x480 32bit resolution.

=~=~=~=

->In This Week's Gaming Section - Surprise: Nintendo s Next Console Is The NES!

"""""""""""""""""""""""""""""""" Independently Developed Game Boy Games Released!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""

Surprise: Nintendo s Next Console Is The NES

Let this tiny box transport you to a time when you didn’t have a job, mortgage, and loud children to distract you.

After years spent letting the software-based Virtual Console largely rot on its vine, Nintendo is trying to cash in on its nostalgia-filled back catalog with a new piece of old hardware. The NES Classic Edition, announced today, is a palm-sized, HDMI-equipped re-release of the ’80s console that will launch on November 11, preloaded with 30 games for $59.99.

We wanted to give fans of all ages the opportunity to revisit Nintendo s original system and rediscover why they fell in love with Nintendo in the first place, Nintendo of America President and COO Reggie Fils-Aime said in a statement. The Nintendo Entertainment System: NES Classic Edition is ideal for anyone who remembers playing the NES, or who wants to pass on those nostalgic memories to the next generation of gamers.

Nintendo hasn’t said much about the underlying hardware powering the re-release, but it doesn’t sound like the new system will be exactly the same as the original. For one thing, the announcement makes no mention of the ability to plug in old NES game cartridges, even though pictures show a familiar, cartridge slot dust-cover styled on the system’s boxy case. For another, Nintendo says that "each game has multiple suspend points, so you can start where you left off at a later time, no passwords needed," suggesting that some sort of virtualized, emulated version of the underlying games is being used.

The new system also will not support old NES controllers natively. Instead, it has slots that will fit the existing Wii Classic Controller Pro and will also work with a new NES Classic Controller patterned after the original rectangular design (sorry dog-bone fans). One Classic Controller will be included with the system; extra ones will retail for $9.99.

Nintendo is coming late to a trend that has hit many other classic consoles in recent years. Sega licensed its old hardware and software for a number of "Arcade Classic" system-on-a-chip Genesis re-releases, most of which have a slot for classic cartridges and support original controllers as well as built-in games. The Atari Flashback line similarly recreates the Atari 2600 and 7800, with some hackers going so far as to add a cartridge port for their decades-old games. Even the Colecovision and Intellivision got Flashback re-releases.

If you have $500+ to spend on a 30-year-old console, this is the one to buy.

Nostalgia-minded Nintendo gamers looking for new hardware, on the other hand, have been stuck settling for gray market Famiclone systems, or emulation-based hardware like the Retron 5, which have their issues when it come to compatibility and authenticity. Then there’s the Analogue Nt, a high-end, high-def, high-priced NES

modification sourced from actual Famicom chips, which we recently reviewed.

Here are the 30 games that will be included on the NES Classic Edition:

Balloon Fight
Bubble Bobble
Castlevania
Castlevania II: Simon s Quest
Donkey Kong
Donkey Kong Jr.
Double Dragon II: The Revenge
Dr. Mario
Excitebike
Final Fantasy
Galaga
Ghosts N’ Goblins
Gradius
Ice Climber
Kid Icarus
Kirby s Adventure
Mario Bros.
Mega Man 2
Metroid
Ninja Gaiden
Pac-Man
Punch-Out!! Featuring Mr. Dream
StarTropics
Super C
Super Mario Bros.
Super Mario Bros. 2
Super Mario Bros. 3
Tecmo Bowl
The Legend of Zelda
Zelda II: The Adventure of Link

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

5 New Independently Developed Game Boy Games Released

The Nintendo Game Boy is a popular hand held. Independent developers seem to love it and we have five new games that were just released for it. Some are from competitions such as bitbitjam and others are just games someone thought would be cool to release.

The Faerie Princess

This is simply a boss battle game. There is a little bit of text

at the beginning to tell you what is going on. Get four hits on the boss without sustaining one yourself and you win. Let one of the fireballs hit you and it is game over. This one is REALLY short. May be good if you are looking for a short game- something similar to the shortness most people experience with Flappy Bird.

Flappy Boy

Okay, are you sick of Flappy Bird clones and the like yet? Judging by the number of people reading the articles we post about them, the videos we make available and general reaction from readers - nope. Remember, we push the content that you, our friends, support. Oh, this is just another Flappy Bird clone - it is tough as nails and annoying as all get out. There was an actual Flappy Bird development jam where this title was developed.

Run to Databay

This is an endless runner, 3D style, game for the Game Boy. Developed for the GBJAM 4 event. If you are easily frustrated then avoid this one- it is as tough in 3D as Flappy Bird is in 2D. Pillars pop up quickly and it is hard to get out of the way in time.

Akaru-hime the Red Princess

This is a rather simple game. Deceptively simple. You are limited to looking left/right and jumping/ducking. You are armed with a sword and have to defend your home from the invading ninjas. There are throwing stars that come flying in rather quickly. Perfect for the older model Game Boy that has severe blur problems. Developed for bitbitjam #3.

Pretty Princess Castle Escape

Here is an extremely tough action platforming game starring the Princess. She is not waiting for an overweight plumber and his brother to come to her rescue. Get ready for frustration and almost throwing your Game Boy on this one. Created for the bitbitjam #3 event.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Snowden Says It’s A ’Dark Day for Russia’ After Putin Signs Anti-Terror Law

Whistleblower and ex-NSA employee Edward Snowden has criticized a new anti-terror law introduced on Thursday by Russian President Vladimir Putin, referring it as "repressive" and noting that it

is a "dark day for Russia."

The new legislation signed by Putin would compel the country's telephone carriers and Internet providers to record and store the private communications of each and every one of their customers for six months and turn them over to the government if requested.

The data collected on customers would include phone calls, text messages, photographs, and Internet activities that would be stored for six months, and "metadata" would be stored up to 3 years.

Moreover, Instant messaging services that make use of encryption, including WhatsApp, Telegram, and Viber, could face heavy fines of thousands of pounds if these services continue to operate in Russia without handing over their encryption keys to the government.

"Putin has signed a repressive new law that violates not only human rights but common sense. A dark day for Russia," Snowden wrote on Twitter.

Snowden is responsible for revealing global mass surveillance programs by leaking NSA classified documents back in June 2013 before finding asylum in Russia.

The activist explained that the new Russian law, in addition to "political and constitutional consequences," would cost telecommunications providers over $30 Billion to implement the new law, which is more than they can afford.

The CEO of Russia s second-largest telecom company Megafon told a local newspaper Thursday that he would rather pay the government higher taxes than spend over $3 Billion yearly on infrastructure upgrades.

"Well be unable to fulfill the requirements of law in the way that it exists at present," said Megafon CEO Sergey Soldatenkov, adding that his company only generates an annual profit of $780 Million.

"When we saw the provisions of the bill, we really hoped that it will not be accepted. I believe we have done everything possible to inform deputies, Federation Council [and] the government that the bill in this form is impossible," Soldatenkov added.

A spokesperson for Tele2, another Russian telecom company, said it might have to raise prices threefold or more in order to accommodate the new law, The WSJ reported.

The Russian government will establish the precise requirements of the new legislation, according to the Kremlin website.

This frightening new legislation comes into force on July 20th.

Bulgaria Passes Law That Mandates Government Software Must Be Open Source

Do you have any idea what the software you have installed is doing stealthily in the background? If it’s not an open source software, can you find out?

Usually, the answer is no.

After Edward Snowden s revelations, it’s clear that how desperately government agencies wants to put secret backdoors in your network, devices, and software.

However, Bulgaria has come forward with an all new set of laws that would be appreciated by privacy lovers and open-source community.

The Bulgarian Parliament has passed legislative amendments to its Electronic Governance Act that require all software written for the country’s government to be fully open-sourced and developed in the public Github repository.

This means that source code of software developed for the Bulgarian government would be accessible to everyone and provided free for use without limitations.

Article 58A of the Electronic Governance Act states that administrative authorities must include the following requirements for procuring software:

"When the subject of the contract includes the development of computer programs, computer programs must meet the criteria for open-source software; all copyright and related rights on the relevant computer programs, their source code, the design of interfaces, and databases which are subject to the order should arise for the principal in full, without limitations in the use, modification, and distribution; and development should be done in the repository maintained by the agency in accordance with Art 7c pt. 18."

However, it does not mean that Bulgaria is going to shift to Linux overnight. It means that whatever computer software, code, databases and programming interfaces the government procures will be freely available for others to read, modify and use, said Bulgarian government adviser Bozhidar Bozhanov.

"Existing solutions are purchased on licensing terms, and they remain unaffected (although we strongly encourage the use of open source solutions for that as well)," Bozhanov said in a blog post.

He added that the decision "is a good step for better government software and less abandonware, and I hope other countries follow our somewhat ’radical’ approach of putting it in the law."

The move will also allow researchers and white hat hackers to report security loopholes and vulnerabilities in government websites that are left unpatched for years, helping the government to detect bad security practices earlier.

However, criminal mind people could also use the flaws for

malicious purpose rather than reporting it to the government.

With the new amendments, Bulgaria becomes the first country to make a law out of open source governance, and we hope that other nations follow this suit.

Oops! TP-Link Forgets To Renew and Loses Its Domains Used To Configure Router Settings

To make the configuration of routers easier, hardware vendors instruct users to browse to a domain name rather than numeric IP addresses.

Networking equipment vendor TP-LINK uses either tplinklogin.net or tplinkextender.net for its routers configuration. Although users can also access their router administration panel through local IP address (i.e. 192.168.1.1).

The first domain offered by the company is used to configure TP-LINK routers and the second is used for TP-LINK Wi-Fi extenders.

Here’s the Blunder:

TP-Link has reportedly "forgotten" to renew both domains that are used to configure its routers and access administrative panels of its devices.

Both domains have now been re-registered using an anonymous registration service by an unknown entity and are being offered for sale online at US$2.5 Million each.

This latest TP-Link oversight, which was first spotted by Cybermoon CEO Amitay Dan, could lead its users to potential problems.

However, it seems like TP-Link is not at all interested in buying back those domains, as Dan claims that the hardware vendor is updating its manuals to remove the domain name references altogether.

In recent years, the hardware vendor has started replacing its tplinklogin.net domain with tplinkwifi.net domain, which is currently under its control. So, there is no direct threat to TP-Link users.

But unfortunately, the tplinklogin.net and tplinkextender.net usually came printed on the back of the devices. So, users accessing this domain on devices could end up on a domain under a third-party’s control.

If malicious actors get their hands on these domains, they could use them to distribute malware, serve phishing pages instructing users to "download new firmware to your router," and request device or social media credentials from users before redirecting them to the router’s local admin panel IP.

The bottom line:

Users are advised to avoid accessing their TP-Link routers using the tplinklogin.net domain; instead, use local IP address.

Dan has also recommended Internet Service Providers (ISPs) to block the affected domain names in order to prevent its customers from being hijacked.

DARPA Challenges Hackers To Create Automated Hacking System Win $2 Million

Why we can t detect all security loopholes and patch them before hackers exploit them?

Because... we know that humans are too slow at finding and fixing security bugs, which is why vulnerabilities like Heartbleed, POODLE and GHOST remained undetected for decades and rendered almost half of the Internet vulnerable to theft by the time patches were rolled out.

Now to solve this hurdle, DARPA has come up with an idea: To build a smart Artificial Intelligence System that will automatically detect and even patch security flaws in a system.

Isn’t it a revolutionary idea for Internet Security?

The Defense Advanced Research Projects Agency (DARPA) has selected seven teams of finalists who will face off in a historic battle, as each tries to defend themselves and find out flaws without any human control.

The DARPA Cyber Grand Challenge will be held at the annual DEF CON hacking conference in Las Vegas next month.

The winner team will be awarded a prize money of $2 Million for building a system that can not only detect vulnerabilities but also write its own patches and deploy them without crashing.

"Cyber Grand Challenge [CGC] is about bringing autonomy to the cyber domain," CGC program manager Mike Walker said in a conference call Wednesday. "What we hope to see is proof that the entire security lifecycle can be automated."

Walker said software bugs go undetected for an average of 312 days, which hackers can often exploit. In fact, even after detecting the flaws, the human takes much time to understand the bugs, develop patches, and then release them to the broader community.

The CGC aims to make this issue much easier, building a system that can sniff out software vulnerabilities and fix them within minutes, or even seconds, automatically.

For Cyber Grand Challenge, the seven teams of finalists will be given a DARPA-constructed computer powered by a thousand Intel Xeon processor cores and 16TB (terabytes) of RAM.

Each team has the task to program their machine with a "cyber reasoning system" that will be able to recognize and understand previously-undisclosed software, detect its flaws, and fix them without human intervention.
Moreover, once the challenge starts, the teams will not be able to jump on their machine’s keyboards and do anything more.

The cyber reasoning systems will be networked in such a way that the teams can also examine their competitors’ systems for issues, but can’t actually hack them, and get extra points if they are able to generate automatically proof-of-concept (POC) exploits for flaws found in their opponents.

The contest will be held at 5 pm on August 4 for over 10 hours in the Paris hotel ballroom in Las Vegas. The first winner team will take home $2 Million in prize money, while the second and third winner will get $1 Million and $750,000, respectively.

After the competition, all the teams’ code, along with DARPA’s own test code, will be made available online under an open-source license.

Corrupt Federal Agent Charged in Silk Road Theft
Accused of Stealing Another $700,000

A former United States undercover agent who stole hundreds of thousands of dollars worth of Bitcoins during an investigation into the underground drug marketplace Silk Road is now suspected of stealing even more of the cryptocurrency from two other cases.

Shaun Bridges is one of two former US agents who pleaded guilty last year and was sentenced in December to almost six years in prison for stealing over $800,000 in Bitcoin while investigating the Darknet marketplace.

Bridges and his partner stole money from Silk Road accounts and framed someone else for it, which lead the Silk Road chief Ross Ulbricht to plan a murder. Ulbricht is now serving life in prison sentence.

Ulbricht was convicted in February 2015 of running the underground black market.

According to court filings unsealed on Thursday, Bridges is believed to have stolen additional funds from a Secret Service account on two different occasions months after he was initially charged.

Bridges and 46-year-old former Drug Enforcement Agency (DEA) special agent Carl Force both were part of Baltimore-based task force to investigate illegal activity in the Silk Road marketplace.

According to an affidavit, the Justice Department came to know in April last year that Bridges might have kept a private encryption key to access a Bitcoin wallet with the $700,000 in BTC that the Silk Road task force had seized in 2014.

The Justice Department urged the Secret Service to move the funds to a different online wallet as a means of protecting it. But when the Secret Service accessed the wallet, all the bitcoins were gone.

"Unfortunately, the U.S. Secret Service did not do so and the funds were thereafter stolen, something the U.S, Secret Service only discovered once it was ordered by a court to pay a portion of the seizure back to affected claimants," prosecutors wrote in an accompanying motion.

The missing bitcoins were found by the agency in December when Bridges was sentenced after admitting that he moved and stole nearly 20,000 Bitcoins (around US$350,000 at the time), the affidavit said.

Bridges later liquidated the stolen Bitcoins into $820,000 between March and May 2013 and transferred all the funds to his personal investment accounts in the United States.

Bridges has started serving his original sentence at the US prison in Terre Haute, Indiana. Though, it is not clear when additional charges will be filed against him.

Attorney Steve Levin of Levin & Curlett LLC is representing Bridges in the case.

Microsoft Fixes Decades-Old Printer Bug in Windows

Printers. They can be the bane of every home office or small business, but not just when they jam or run out of paper or toner. They can also spread malware to systems connected to them.

Microsoft this week published a fix for a printer vulnerability that has existed in the Windows family since Windows 95. However, Microsoft hasn’t really plugged the hole; instead, it added a warning to Windows as part of its most recent patch cycle, which will now let you know if you’re installing "untrusted" printer drivers. Presumably, that will prevent you from doing so.

"The vulnerability in question centers on the ways that network users find and use printers on a network. Needless to say, modern organizations often have many users, and likewise often have many different makes and models of printers. Users expect to connect to and use whatever printer is most convenient, and likewise, mobile users expect to be able to come in to the office and print," reads a blog post from security firm Vectra Networks, which investigated the vulnerability alongside Microsoft.

"To serve these users, organizations need a way to deliver the necessary printer drivers to the users who need them. Instead of pushing every possible driver to all users, many networks use the Microsoft Web Point-and-Print (MS-WPRN) approach that allows a user to connect to any printer on the network, and have the printer or print server deliver the appropriate driver on demand. To make this as easy and seamless as possible, these drivers are

often delivered without a warning or triggering User Account Controls (UAC)."

The primary problem is that an attacker could compromise a printer a not-so-secure device, Vectra notes which would then allow the printer to act as a distribution center for malware disguised as system-level printer drivers. The attacker then gains a great deal of access to the infected system, as well as an easy way to spread the malware to anyone else foolish enough to try connecting to the printer.

An intrepid attacker might not even need to infect an actual printer. All the person would need is a network-equipped device (like a laptop) that can pretend it’s a printer. That, or an attacker could simply wait for a legitimate driver request to a legitimate network printer, but throw down a man-in-the-middle attack that responds with malware disguised as drivers.

Or, in one extreme case, an attacker might not even need to have physical access to one’s local network at all.

"Thus far, you may be feeling relatively safe because all of this supposes that the attacker is already on your network. However, the same mechanism works over the Internet using the Internet Printing Protocol and webPointNPrint. This opens the door to infections being delivered over the Internet via normal Web-based vectors such as compromised websites or ads. A bit of javascript in an advertisement could easily trigger a request to a remote ’printer’ that would then deliver the malicious driver to the victim. Using both of these approaches, an attacker could both infect a user from the outside and then use his newly gained internal position to spread laterally within the network," Vectra notes.

Microsoft also issued bug fixes for products like Edge and Internet Explorer, as well as Adobe Flash.

Facebook s OpenCellular Is A New Open-source Wireless Access Platform for Remote Areas

Facebook is clearly very serious about its mission to connect the world and in the process, it has launched solar-powered drones that use lasers to connect to each other and the ground, and more prosaic efforts like new antennas for covering both urban and rural areas. Today, Facebook is expanding this work with the launch of OpenCellular, a new open source hardware and software project that aims to bring a more affordable wireless access platform to remote areas.

One of the reasons the expansion of cellular networks has stalled is that the ecosystem is constrained, Facebook engineer Kashif Ali writes. Traditional cellular infrastructure can be very expensive, making it difficult for operators to deploy it everywhere and for smaller organizations or individuals to solve hyperlocal connectivity challenges. It s often unaffordable for them to attempt to extend network access in both rural and developed communities.

Ali previously co-founded Endaga, which worked on a somewhat similar project. Facebook acquired the company last October. He also notes that one of the goals of the projects was to build a system with very little physical footprint and the ability to use already available infrastructure because the cost of the land, tower, power and security for setting up a cellular network is often higher than that of the actual access point itself.

Facebook says OpenCellular will consist of two main subsystems: one for general purpose and base-band computing, and one to handle the actual radio. Both of those systems were designed to be somewhat modular. The radio system, for example, could be based on a software-defined radio or on a system-on-chip solution. While the focus here is on providing wireless access to the Internet over anything from a 2G to LTE network, OpenCellular could also be used to provide a local network, too.

These devices will likely be deployed in rather harsh conditions, so both the industrial and mechanical design aims to make them rugged enough to withstand high winds and extreme temperatures while still being small enough to be deployed by a single person.

Facebook says it will open source the hardware design, firmware and control software for OpenCellular so telecom operators, entrepreneurs, researchers and OEMs will be able to build their own versions. It will also donate the work to the Telecom Infra Project, a Facebook-backed initiative for exploring new approaches to well telecom infrastructure basics like access and backhaul.

Along with tackling connectivity trouble in the developing world, Facebook is also trying to make it easier for them to access rich media. Today it announced a test of video downloads in India to enable offline viewing. Facebook wants everyone, no matter where, on its social network.

I’m Warning You, Don’t Read this Article. It’s A Federal Crime!

Yes, you heard it right. If I tell you not to visit my website, but you still visit it knowing you are disapproved, you are committing a federal crime, and I have the authority to sue you.

Wait! I haven’t disapproved you yet. Rather I’m making you aware of a new court decision that may trouble you and could have big implications going forward.

The United States Court of Appeals for the Ninth Circuit has taken a critical decision on the Computer Fraud and Abuse Act (CFAA): Companies can seek civil and criminal penalties against people who access or visit their websites without their permission.

Even Sharing Password is also a Federal Crime...

Yes, a similar weird decision was taken last week when the Ninth Circuit Court of Appeals ruled that sharing passwords can be a

violation of the CFAA, making Millions of people who share their passwords "unwitting federal criminals."

Now, you might be wondering how visiting a publically open website could be a crime. Well, there’s a legal battle behind it:

CASE: Facebook Vs. Power Ventures

The case involves a start-up called Power Ventures allows its users to log-in and manage all of their social network accounts from one place claimed on its site that the "First 100 people who bring 100 new friends to Power.com win $100."

Once clicked on the link, Power used a service that let users fetch all of their contacts on different social media sites to send a series of promotional emails and internal Facebook messages inviting their friends to sign-up on Power.com.

On discovering the activity, Facebook blocked the Power’s API app to access its website and user’s data, as well as sent a cease-and-desist letter to the scammy service telling the company to stop.

"Facebook does allow third parties to access content by enrolling in the site’s Facebook Connect program, but Power never registered with the system and conducted activities beyond the program s scope," says Orin Kerr, Professor of law at the George Washington University Law School.

According to the cease-and-desist letter, Power was violating Facebook’s terms of use that may have violated federal and state law.

Even being explicitly warned to stop, Power continued using Facebook s website, which forced Facebook to sue Power Ventures in the year 2008 for violating Computer Fraud and Abuse Act (CFAA).

In September 2013, the federal court ordered Power to pay more than $3 Million in damages to Facebook on the ground that Power had violated CFAA Law.

The case was pending before the Ninth Circuit, who has also sided with Facebook recently.

Well, I’m not convinced. The court ruling is really too broad that gives prosecutors too much power to turn your activities, such as password sharing and visiting websites, into federal crimes.

Microsoft Wins Appeal in Dublin Datacenter Warrant Case

A federal appeals court today overturned a lower court ruling ordering Microsoft to turn over the contents of e-mails stored in an offshore datacenter. The decision is a major victory for Microsoft and all major cloud and data services providers

seeking to ensure user data is protected under the laws of the countries where information is stored.

The closely watched case centered around Microsoft's refusal to comply with a search warrant by U.S. law enforcement demanding that it turn over the contents of specific e-mails residing in its Dublin, Ireland datacenter in connection with a criminal investigation. While Microsoft did turn over the data in its U.S. datacenters, the company argued that complying with the search warrant's demand to provde the e-mails was beyond the scope of U.S. law. Despite support from Apple, AT&T, Cisco and Verizon, along with the Electronic Frontier Foundation, the U.S. District Court for the Southern District of New York upheld the search warrant issued nearly two years ago. Microsoft subsequently filed the appeal last year arguing privacy laws superseded the court's ruling. "This case is about how we best protect privacy, ensure that governments keep people safe and respect national sovereignty while preserving the global nature of the Internet," Microsoft President and Chief Legal Officer Brad Smith stated at the time.

Smith hailed today's decision as a key precedent for privacy. "It ensures that people's privacy rights are protected by the laws of their own countries; it helps ensure that the legal protections of the physical world apply in the digital domain; and it paves the way for better solutions to address both privacy and law enforcement needs," Smith stated in a blog post.

A panel of three appeals court judges from the U.S. Court of Appeals for the Second Circuit found that last year's ruling ordering Microsoft to comply with a search warrant was invalid, noting that search warrants carried out by U.S. law enforcements are typically limited to locations within this country's borders or locations it has jurisdiction over, according to the ruling. Warrants don't traditionally extend further.

"Because Microsoft has complied with the Warrant's domestic directives and resisted only its extraterritorial aspects, we REVERSE the District Court's denial of Microsoft's motion to quash, VACATE its finding of civil contempt, and REMAND the cause with instructions to the District Court to quash the Warrant insofar as it directs Microsoft to collect, import, and produce to the government customer content stored outside the United States, according to the ruling.

Smith yesterday gave a speech at Microsoft's Worldwide Partner Conference in Toronto where he gave an impassioned emphasis on the company's commitment to fighting for customer privacy and spoke to this closely watched case. "We need an Internet that respects people's rights," he said. "We need an Internet that is governed by law [and] we need an Internet that's governed by good law."

Smith has been a vocal proponent that the Communications Storage Act under the Electronic Privacy Act of 1986 is based on is dated and has urged Congress and the White House to create laws that are consistent with the modern world. Apparently the appeals court agreed as noted in the ruling: "Three decades ago, international boundaries were not so routinely crossed as they are today, when service providers rely on worldwide

networks of hardware to satisfy users' 21st century demands for access and speed and their related, evolving expectations of privacy."

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.